

⑫ 公開特許公報(A)

平2-44389

⑬ Int.Cl.⁹

識別記号

庁内整理番号

⑭ 公開 平成2年(1990)2月14日

G 09 C 1/00
G 08 K 17/00
19/10

S

7368-5B
6711-5B

6711-5B G 06 K 19/00

R

審査請求 未請求 請求項の数 3 (全9頁)

⑮ 発明の名称 ICカード機器

⑯ 特 願 昭63-194988

⑰ 出 願 昭63(1988)8月4日

⑱ 発 明 者 伊 藤 守 大阪府門真市大字門真1006番地 松下電器産業株式会社内
 ⑲ 発 明 者 高 木 伸 哉 大阪府門真市大字門真1006番地 松下電器産業株式会社内
 ⑳ 出 願 人 松下電器産業株式会社 大阪府門真市大字門真1006番地
 ㉑ 代 理 人 弁理士 栗野 重孝 外1名

明 細 書

1、発明の名称

ICカード機器

2、特許請求の範囲

(1) 第1のICカード装置と、この第1のICカード装置と交信する第2のICカード装置とを備え、前記第1のICカード装置は、乱数を発生するための第1の乱数発生手段と、前記第1の乱数発生手段から得られる乱数を暗号化するための第1の暗号化手段と、外部から入力される暗号化データを復号化するための第2の復号化手段と、前記第2の復号化手段から得られるデータを第1のデータと第2のデータに分離するためのデータ分離手段と、前記データ分離手段から得られる第2のデータを暗号化するための第3の暗号化手段と、前記第1の乱数発生手段から得られる乱数と前記データ分離手段から得られる第1のデータを比較するための第1の比較手段と、データの入出力、記憶、演算などのデータ処理を行なう第1の処理手段と、前記

データ分離手段から得られる第2のデータと前記第1の乱数発生手段から得られる乱数を用いて前記第1の処理手段から送出されるデータを暗号化し、外部から入力される暗号化データを復号化するための第1の通信手段とを有し、前記第2のICカード装置は、乱数を発生するための第2の乱数発生手段と、外部から入力される暗号化データを復号化するための第1の復号化手段と、前記第2の乱数発生手段から得られる乱数と前記第1の復号化手段から得られるデータを連結するためのデータ連結手段と、前記データ連結手段から得られる連結データを暗号化するための第2の暗号化手段と、外部から入力される暗号化データを復号化するための第3の復号化手段と、前記第2の乱数発生手段から得られる乱数と前記第3の復号化手段から得られるデータを比較するための第2の比較手段と、データの入出力、記憶、演算などのデータ処理を行なう第2の処理手段と、前記第1の復号化手段から得られるデータと前記第2の乱数発生手段から得られる乱数を用いて外部から

入力される暗号化データを復号化し、前記第2の処理手段から送出されるデータを暗号化するための第2の通信手段とを有する構成としたICカード機器。

(2) 第1のICカード装置に装着される第3のICカード装置は、第1の乱数発生手段と第1の暗号化手段と第2の復号化手段と第3の暗号化手段とデータ分離手段と第1の比較手段から構成される請求項1記載のICカード機器。

(3) 第2のICカード装置に装着される第4のICカード装置は、第2の乱数発生手段と第1の復号化手段と第2の暗号化手段と第3の復号化手段とデータ連結手段と第2の比較手段から構成される請求項1記載のICカード機器。

3. 発明の詳細な説明

産業上の利用分野

本発明は、第1のICカード装置(例えば主として情報を記憶する集積回路がカード内に組み込まれたICカード)と、そのICカードと情報の交換を行う第2のICカード装置(例えばカード端末)とから構成されるICカード機器に関する

の関数演算F2を行うための第2の演算手段452と、データの入出力、記憶、演算などのデータ処理を行う第2の処理手段456と、第1の復号化鍵KD1を用いてカード端末400から入力される暗号化データを復号化するための第1の復号化手段454と、第2の暗号化鍵KE2を用いて前記第2の処理手段456から送出されるデータを暗号化するための第2の暗号化手段455とを備えている。

このように構成された従来のICカード機器について、その動作を以下に説明する。

ICカード450がカード端末400に挿入されると情報の交換を行う前に、カード端末400はICカード450の正当性(偽造されていないこと)を確認するため、乱数発生手段401から乱数Rを生成し、ICカード450に送信する。ICカード450が受信した乱数Rは第2の演算手段452に入力され、ICカード450内に記憶されている第2の秘密データK2とあらかじめ定められた関数演算F2が施されてカード端末

ものである。

従来の技術

第4図は従来例を示したものである。

第4図において、カード端末400は、乱数Rを生成するための乱数発生手段401と、第1の秘密データK1と前記乱数発生手段401から得られる乱数Rと関数演算F1を行うための第1の演算手段402と、前記第1の演算手段402から得られるデータとICカード450から入力されるデータとを比較するための比較手段403と、データの入出力、記憶、演算などのデータ処理を行う第1の処理手段406と、第1の暗号化鍵KE1を用いて前記第1の処理手段406から送出されるデータを暗号化するための第1の暗号化手段404と、第2の復号化鍵KD2を用いてICカード450から入力される暗号化データを復号化するための第2の復号化手段405とを備えている。一方、カード端末400と情報の交換を行うICカード450は、第2の秘密データK2とカード端末400から入力される乱数Rと

400に送信され、カード端末400内の比較手段403に入力される。

一方、カード端末400ではICカード450と同様に、乱数発生手段401から得られる乱数Rは第1の演算手段402に入力され、カード端末400内に記憶されている第1の秘密データK1とあらかじめ定められた関数演算F1が施され、比較手段403に入力される。第1と第2の演算手段402、452が同一の関数演算を行い、第1と第2の秘密データが同一のデータであれば、比較手段403に入力される二つのデータは同一の値を持つ。比較手段403は、入力された二つのデータを比較し、両者が一致している時に限り、カード端末400はICカード450を正当なICカードであると判断して、第1の処理手段406に対してICカード450との情報の交換を許可する。

情報の交換を許可された第1の処理手段406は第1の暗号化手段404に対して送信データを送出し、第1の暗号化手段404はカード端末

400に記憶されている第1の暗号化鍵 K_1 を用い、入力された送信データを暗号化してICカード450に送信する。ICカード450が受信した暗号化データは第1の復号化手段454に入力され、ICカード450内に記憶されている第1の復号化鍵 K_1 を用いて復号化され、第2の処理手段456に入力される。

また、第2の処理手段456は第2の暗号化手段455に送信データを送出し、第2の暗号化手段455はICカード450内に記憶されている第2の暗号化鍵 K_2 を用いて暗号化し、カード端末400に送信する。カード端末400が受信した暗号化データは第2の復号化手段406に入力され、カード端末400内に記憶されている第2の復号化鍵 K_2 を用いて復号化され、第1の処理手段408に入力される。以上のように、暗号化処理と復号化処理の繰り返しにより、カード端末400とICカード450との間で情報の交換が行われる。

発明が解決しようとする課題

また、情報の交換については、あらかじめカード端末400とICカード450に記憶されている暗号化鍵と復号化鍵を用いて、交換しようとする情報の暗号化処理と復号化処理を行いながらカード端末400とICカード450間で通信を行うため、暗号化処理と復号化処理において同一の暗号アルゴリズムと同一の鍵が長期間使用されると暗号が解読され、通信情報が漏洩する危険性があった。

これらの問題点を解決するためには、カード端末400とICカード450の両方に記憶されている秘密データや暗号化鍵、復号化鍵を頻繁に取り換える必要があるが、ICカード450は不特定多数のユーザに所持されることが多いため、現実的には秘密データや暗号化鍵、復号化鍵の取り換えはかなり困難である。

本発明はこのような課題に鑑み、秘密データや暗号化鍵、復号化鍵を頻繁に取り換えることなく、ICカードの正当性が確認でき、また、安全にICカードとカード端末の間で情報の交換が行な

このような従来のICカード機器において、まずICカード450がカード端末400の正当性を確認できないという問題点があった。この問題点については、ICカード450がカード端末400と同様な乱数発生手段と比較手段とを具備すれば、カード端末400がICカード450の正当性を確認する方法と同様にICカード450がカード端末400の正当性を確認することができ、容易に解決することができる。

しかしながら、このような従来のICカード機器においては、カード端末400がICカード450の正当性を確認するために生成した乱数 R と、その乱数 R を第2の演算手段452で演算した結果 $F_2(R, K_2)$ とが端末とICカードのインタフェース部に毎回あらわれるため、第三者が乱数 R とその演算結果 $F_2(R, K_2)$ のペアを容易に入手することが可能となり、万一、関数演算のアルゴリズムが漏洩すると、秘密データが解読される恐れがあり、ICカードが偽造される危険性があった。

えるようなICカード機器を提供することを目的としている。

課題を解決するための手段

上記目的を達成するため、本発明は、第1のICカード装置は、乱数を発生するための第1の乱数発生手段と、前記第1の乱数発生手段から得られる乱数を暗号化するための第1の暗号化手段と、外部から入力される暗号化データを復号化するための第2の復号化手段と、前記第2の復号化手段から得られるデータを第1のデータと第2のデータに分離するためのデータ分離手段と、前記データ分離手段から得られる第2のデータを暗号化するための第3の暗号化手段と、前記第1の乱数発生手段から得られる乱数と前記データ分離手段から得られる第1のデータを比較するための第1の比較手段と、データの入出力、記憶、演算などのデータ処理を行う第1の処理手段と、前記データ分離手段から得られる第2のデータと前記第1の乱数発生手段から得られる乱数を用いて前記第1の処理手段から送出されるデータを暗号化

し、外部から入力される暗号化データを復号化するための第1の通信手段とを備えたものとし、第2のICカード装置は、乱数を発生するための第2の乱数発生手段と、外部から入力される暗号化データを復号化するための第1の復号化手段と、前記第2の乱数発生手段から得られる乱数と前記第1の復号化手段から得られるデータを連結するためのデータ連結手段と、前記データ連結手段から得られる連結データを暗号化するための第2の暗号化手段と、外部から入力される暗号化データを復号化するための第3の復号化手段と、前記第2の乱数発生手段から得られる乱数と前記第3の復号化手段から得られるデータを比較するための第2の比較手段と、データの入出力、記憶、演算などのデータ処理を行なう第2の処理手段と、前記第1の復号化手段から得られるデータと前記第2の乱数発生手段から得られる乱数を用いて外部から入力される暗号化データを復号化し、前記第2の処理手段から送出されるデータを暗号化するための第2の通信手段とを備えたものにしたもの

いて復号化し、連結データを得る。カード端末はこの連結データを二つの乱数データに分離し、このうちICカードが生成したと推定される乱数データをあらかじめカード端末に記憶されている暗号化鍵で暗号化してICカードに送信し、一方のカード端末が生成したと推定される乱数データをカード端末が実際に生成した乱数データと比較する。また、ICカードは、受信した暗号化データをあらかじめICカード内に記憶されている復号化鍵で復号化し、この復号化データをICカードが実際に生成した乱数データと比較する。

カード端末において、カード端末が生成したと推定される乱数データとカード端末が実際に生成した乱数データとが一致するためには、カード端末が生成した乱数データがICカード内で正しく復号化及び暗号化される必要があり、こういう処理が可能なICカードは正当な手段で配送された復号化鍵と暗号化鍵を有していると考えられ、カード端末にとって正当なICカードであると判断できる。またICカードにおいて、カード端末か

である。

作用

本発明は上記した構成により、第2のICカード装置(例えばICカードで以下、IOカードと記する)が第1のICカード装置(例えばカード端末で以下、カード端末と記する)に挿入されると、カード端末は乱数データを生成し、これをカード端末内にあらかじめ記憶されている暗号化鍵で暗号化してICカードに送信する。ICカードは受信した暗号化データをICカード内にあらかじめ記憶されている復号化鍵で復号化し、カード端末が生成した乱数データと同一であると推定される乱数データを得る。さらに、ICカードはICカード内でも乱数データを生成し、生成した乱数データとカード端末が送信してきた乱数データとを連結し、IOカード内にあらかじめ記憶されている暗号化鍵で暗号化してカード端末に送信する。

カード端末は、受信した暗号化データをあらかじめカード端末内に記憶されている復号化鍵を用

ら受信し復号化したデータとIOカードが実際に生成した乱数データとが一致するためには、ICカードが生成した乱数データがカード端末内で正しく復号化及び暗号化される必要があり、こういう処理が可能なカード端末は正当な手段で配送された復号化鍵と暗号化鍵を有していると考えられ、ICカードにとって正当な端末であると判断してよい。

このとき、カード端末とICカードのインタフェース部には、カード端末とICカードが生成した二つの乱数データをそれぞれ暗号化したものと前記二つの乱数データを連結したデータを暗号化したものしかあらわれない。従って、第三者にこれらの暗号化データが入手されても、カード端末もしくはIOカードで生成される乱数データが入手できないため、暗号化鍵を推定するのはきわめて困難であり、長期間にわたって同一の暗号化鍵を使用することができる。

以上のプロセスによりIOカードとカード端末との互いの正当性が確認されると、カード端末と

ICカードはそれぞれが生成し、秘密に交換した二つの乱数データを用いて互いに暗号化処理と復号化処理を繰り返しながら、カード端末とICカードの間で暗号による情報の交換を行う。ICカードがカード端末に挿入されるたびに生成される乱数データを暗号化鍵と復号化鍵に用いているため、鍵を頻繁に取り換えることなく安全に情報の交換を行うことができる。

実施例

以下本発明の実施例について、図面を参照しながら説明する。

(実施例1)

第1図は、本発明のICカード端末装置の第1の実施例を示すブロック図である。

第1図において、110はカード端末100に挿入された取引用ICカード150の正当性を確認するためにカード端末100内に装着された認証用ICカードである。111は乱数データR0を発生するための第1の乱数発生手段、112は認証用ICカード110内に記憶されている第1

から得られる乱数データR0を用いて前記第1の処理手段120から送出されるデータを暗号化し、外部から入力される暗号化データを復号化するための第1の通信手段で、以上から第1のICカード装置としてのカード端末100が構成されている。なお、第1の乱数発生手段111と第1の暗号化手段112と第2の復号化手段と第3の暗号化手段114とデータ分離手段115と第1の比較手段116とは、認証用ICカード110内に構成され、カード端末100の一部として機能している。

また、151は乱数データS0を発生するための第2の乱数発生手段、152は取引用ICカード150内に記憶されている第1の復号化鍵KD1を用いて外部から入力される暗号化データを復号化するための第1の復号化手段である。155は前記第2の乱数発生手段151から得られる乱数データS0と前記第1の復号化手段152から得られるデータR1を連結するためのデータ連結手段、151は取引用ICカード150内に記憶さ

る暗号化鍵KE1を用いて前記第1の乱数発生手段111から得られる乱数データR0を暗号化するための第1の暗号化手段である。113は認証用ICカード110内に記憶されている第2の復号化鍵KD2を用いて外部から入力される暗号化データを復号化するための第2の復号化手段、

115は前記第2の復号化手段113から得られるデータを第1のデータR2と第2のデータS1に分離するためのデータ分離手段である。114は認証用ICカード110内に記憶されている第3の暗号化鍵KE3を用いて前記データ分離手段115から得られる第2のデータS1を暗号化するための第3の暗号化手段である。116は前記第1の乱数発生手段111から得られる乱数データR0と前記データ分離手段115から得られる第1のデータR2を比較するための第1の比較手段である。120はデータの入出力、記憶、演算などのデータ処理を行う第1の処理手段である。130は前記データ分離手段115から得られる第2のデータS1と前記第1の乱数発生手段111

れている第2の暗号化鍵KE2を用いて前記データ連結手段155から得られる連結データを暗号化するための第2の暗号化手段である。154は取引用ICカード150内に記憶されている第3の復号化鍵KD3を用いて外部から入力される暗号化データを復号化するための第3の復号化手段、155は前記第2の乱数データ発生手段151から得られる乱数データS0と前記第3の復号化手段154から得られるデータS2を比較するための第2の比較手段である。160はデータの入出力、記憶、演算などのデータ処理を行う第2の処理手段、170は前記第1の復号化手段152から得られるデータR1と前記第2の乱数発生手段151から得られる乱数データS0を用いて外部から入力される暗号化データを復号化し、前記第2の処理手段160から送出されるデータを暗号化するための第2の通信手段で、以上から第2のICカード装置としての取引用ICカード150が構成されている。上記のように構成されたICカード装置について、以下その動作を説明する。

まず、認証用ICカード110が装着されたカード端末100に取引用ICカード150が挿入されると、認証用ICカード110内の第1の乱数発生手段111は乱数データR0を生成し、第1の暗号化手段112は認証用ICカード110にあらかじめ記憶されている第1の暗号化鍵K1を用いて前記第1の乱数発生手段111から得られる乱数データR0を暗号化して取引用ICカード150に送信する。取引用ICカード150内の第1の復号化手段152は受信した暗号化データを取引用ICカード150内にあらかじめ記憶されている第1の復号化鍵KD1で復号化し、認証用ICカード110が生成した乱数データR0と同一であると推定される乱数データR1を得る。

次に、取引用ICカード150においても第2の乱数発生手段151が乱数データS0を生成し、データ連結手段155は第2の乱数発生手段151から得られる乱数データS0と第1の復号化手段152から得られる乱数データR1との連結処理を行い、連結データR1||S0を生成する。こ

また、第3の復号化手段154は取引用ICカード150が受信した暗号化データをあらかじめ取引用ICカード150内に記憶されている第3の復号化鍵KD3を用いて復号化し、第2の比較手段156は取引用ICカード150で生成されたと推定される乱数データS2と第2の乱数発生手段151から得られる実際に生成した乱数データS0の値を比較する。

第1の比較手段116において、認証用ICカード110が生成したと推定される乱数データR2と第1の乱数発生手段111から得られる実際に生成した乱数データR0との比較結果が第1の処理手段120に対する第1の制御信号C1となる。両データが一致すると、第1の比較手段116は第1の処理手段120に対して取引用ICカード150との情報交換を許可し、不一致のときは情報の交換を禁止する。第2の比較手段156においても同様に、取引用ICカード150で生成されたと推定される乱数データS2と第2の乱数発生手段151から得られる実際に生成し

て、「||」の記号は二つのデータを連結することを意味する。第2の暗号化手段153はこの連結データR1||S0を取引用ICカード150内にあらかじめ記憶されている第2の暗号化鍵K2を用いて暗号化し、カード端末100に送信する。

第2の復号化手段113はカード端末100が受信した暗号化データをあらかじめ認証用ICカード110内に記憶されている第2の復号化鍵KD2で復号化し、取引用ICカード150が生成したと推定される連結データR2||S1を得る。データ分離手段115はこの連結データを二つの乱数データR2、S1に分離し、第3の暗号化手段114は取引用ICカード150が生成したと推定される乱数データS1をあらかじめ認証用ICカード110内に記憶されている第3の暗号化鍵K3で暗号化して取引用ICカード150に送信し、第1の比較手段116は認証用ICカード110が生成したと推定される乱数データR2と第1の乱数発生手段111から得られる実際に生成した乱数データR0の値を比較する。

た乱数データS0との比較結果が第2の処理手段160に対する第2の制御信号C2となり、両データが一致しているときに限り第2の処理手段160に対して情報の交換を許可する。

情報の交換が許可された第1の処理手段120は第1の通信手段130に対して送信データを送出し、第1の通信手段130はデータ分離手段115から得られる乱数データS1と第1の乱数発生手段111から得られる乱数データR0を用い、入力された送信データを暗号化して取引用ICカード150に送信する。取引用ICカード150が受信した暗号化データは第2の通信手段170に入力され、第1の復号化手段152から得られる乱数データR1と第2の乱数発生手段151から得られる乱数データS0を用いて復号化され、第2の処理手段160に入力される。

同様に、情報の交換が許可された第2の処理手段150は第2の通信手段170に対して送信データを送出し、第2の通信手段170は第1の復号化手段152から得られる乱数データR1と第

2の乱数発生手段151から得られる乱数データS0を用い、入力された送信データを暗号化してカード端末100に送信する。カード端末100が受信した暗号化データは第1の通信手段130に入力され、データ分離手段115から得られる乱数データS1と第1の乱数発生手段111から得られる乱数データR0を用いて復号化され、第1の処理手段120に入力される。

以上のように、認証用ICカード110と取引用ICカード150がそれぞれ生成し、秘密に交換した二つの乱数データを用いて互いに暗号化処理と復号化処理を繰り返すことにより、カード端末100と取引用ICカード150の間で安全に情報の交換を行うことができる。

第3図は、第1の実施例における第1と第2の通信手段の一実施例を示すブロック図である。

第3図において、131は第1の処理手段120から送出される送信データを暗号化して取引用ICカード150に送信するための第4の暗号化手段、132はカード端末100が受信した暗号

化データを復号化し第1の処理手段120に入力するための第5の復号化手段で、以上から第1の通信手段130が構成されている。また、171は取引用ICカード150が受信した暗号化データを復号化し第2の処理手段160に入力するための第4の復号化手段、172は第2の処理手段160から送出される送信データを暗号化してカード端末100に送信するための第5の暗号化手段で、以上から第2の通信手段170が構成されている。

第3図の実施例では、第4の暗号化手段131と第4の復号化手段171に、認証用ICカード110で生成された乱数データが暗号化鍵と復号化鍵に用いられ、第5の復号化手段132と第5の暗号化手段172に、取引用ICカード150で生成された乱数データが復号化鍵と暗号化鍵に用いられている。

(実施例2)

第2図は、本発明のICカード端末装置の第2の実施例を示すブロック図である。

第2図において、200はカード端末、210は認証用ICカード、211は第2の乱数発生手段、212は第1の復号化手段、213は第2の暗号化手段、214は第3の復号化手段、215はデータ分離手段、216は第2の比較手段である。220は第2の処理手段、230は第2の通信手段、250は取引用ICカード、251は第1の乱数発生手段、252は第1の暗号化手段、253は第2の復号化手段、254は第3の暗号化手段、255はデータ分離手段、256は第1の比較手段、260は第1の処理手段、270は第1の通信手段で、以上は第1図の構成と同様のものである。

第1図の構成と異なるのは、認証用ICカード210が第2の乱数発生手段211と第1の復号化手段212と第2の暗号化手段213と第3の復号化手段214とデータ連結手段215と第2の比較手段216とから構成され、取引用ICカード250が第1の乱数発生手段251と第1の暗号化手段252と第2の復号化手段253と第

3の暗号化手段254とデータ分離手段255と第1の比較手段256とから構成されている点である。

上記のように構成されたICカード装置について、以下その動作を説明する。

まず、認証用ICカード210が装着されたカード端末200に取引用ICカード250が挿入されると、取引用ICカード250内の第1の乱数発生手段251は乱数データR0を生成し、第1の暗号化手段252は第1の暗号化鍵K1を用いて第1の乱数発生手段251から得られる乱数データR0を暗号化し、カード端末200に送信する。認証用ICカード210内の第1の復号化手段212はカード端末200が受信した暗号化データを第1の復号化鍵KD1で復号化し、取引用ICカード250が生成した乱数データR0と同一であると推定される乱数データR1を得る。

次に、認証用ICカード210においても、第2の乱数発生手段211が乱数データS0を生成し、データ連結手段215は第2の乱数発生手段

211 から得られる乱数データ S0 と第1の復号化手段212 から得られる乱数データ R1 との連結処理を行い、連結データ S0 || R1 を生成する。第2の暗号化手段213 はこの連結データ S0 || R1 を第2の暗号化鍵 K2 を用いて暗号化し、取引用 IC カード 260 に送信する。

第2の復号化手段253 は受信した暗号化データを第2の復号化鍵 K2 で復号化し、認証用 IC カード 210 が生成したと推定される連結データ S1 || R2 を得る。データ分離手段255 はこの連結データを二つの乱数データ S1, R2 に分離し、第3の暗号化手段254 は認証用 IC カード 210 が生成したと推定される乱数データ S1 を第3の暗号化鍵 K3 で暗号化してカード端末200 に送信し、第1の比較手段256 は取引用 IC カード 260 が生成したと推定される乱数データ R2 と第1の乱数発生手段251 から得られる実際に生成した乱数データ R0 の値を比較する。

また、第3の復号化手段214 はカード端末

200 が受信した暗号化データをあらかじめ第3の復号化鍵 K3 を用いて復号化し、第2の比較手段216 は認証用 IC カード 210 で生成されたと推定される乱数データ S2 と第2の乱数発生手段211 から得られる実際に生成した乱数データ S0 の値を比較する。

第1と第2の比較手段256, 216 において各乱数データの値が一致すると、それぞれ第1と第2の処理手段260, 220 に対して情報の交換を許可し、不一致のときには情報の交換を禁止する。各乱数データが一致し情報の交換が許可されると、第1の実施例とまったく同様に、第1と第2の処理手段260, 220 は、第1と第2の通信手段270, 230 を介して暗号通信による情報の交換を行う。

発明の効果

以上述べてきたように、本発明は、第1と第2の IC カード装置に乱数発生手段と暗号化手段と復号化手段を設けることにより、互いの正当性を確認するために生成する乱数を暗号化処理と復号

化処理の鍵に用いることができるため、鍵を頻繁に取り換えることなく、安全に第1と第2の IC カード装置間で情報の交換を行うことができ、きわめて優れた IC カード装置を実現することができる。

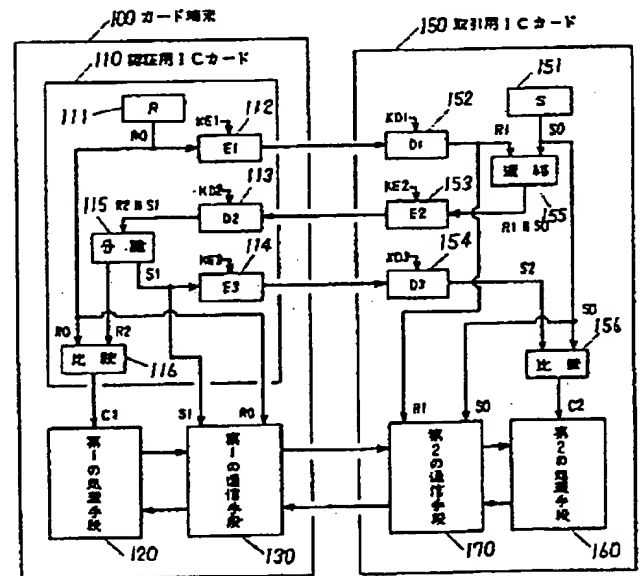
4. 図面の簡単な説明

第1図は本発明の第1の実施例における IC カード装置のブロック図、第2図は本発明の第2の実施例における IC カード装置のブロック図、第3図は本発明の第1の実施例における通信手段のブロック図、第4図は従来の IC カード装置のブロック図である。

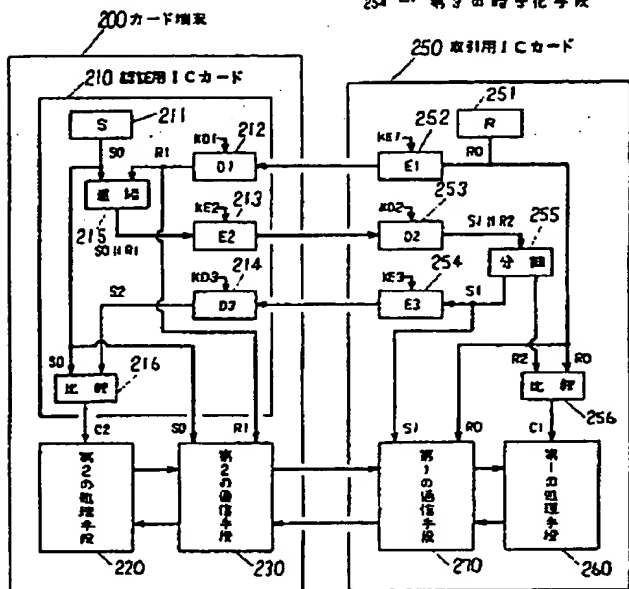
111 ……第1の乱数発生手段、112 ……第1の暗号化手段、113 ……第2の復号化手段、114 ……第3の暗号化手段、151 ……第2の乱数発生手段、152 ……第1の復号化手段、153 ……第2の暗号化手段、154 ……第3の復号化手段。

代理人の氏名 弁理士 栗 野 重 孝 ほか1名

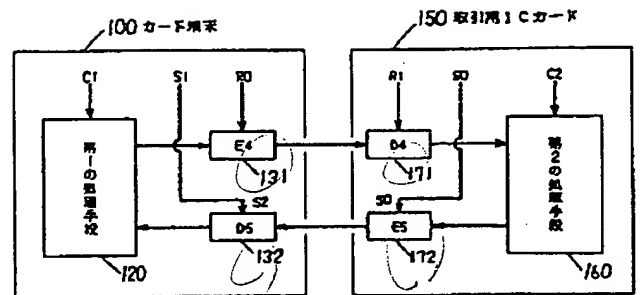
第 1 図



第 2 図



第 3 図



第 4 図

